

Amendments to the Claims

1 Claim 1 (currently amended): In a computing environment having a connection to a network, a
2 computer program product for securely propagating security credentials using a trusted
3 authenticating domain, the computer program product embodied on one or more computer-
4 readable media and comprising:

5 computer-readable program code means for establishing a secure connection between a
6 client and a password synchronization agent (PSA);

7 computer-readable program code means for receiving, at the PSA from the client over the
8 secure connection, transmitting an identifier of a user and an identifying secret of the user from
9 the client to the PSA over the secure connection during propagation request processing;

10 computer-readable program code means for validating the user with the trusted
11 authenticating domain using the ~~transmitted~~ received user identifier and identifying secret, on
12 request of the PSA; and

13 computer-readable program code means for propagating the received identifying secret of
14 the user directly from the PSA to a master registry if the validation succeeds.

1 Claim 2 (original): The computer program product according to Claim 1, further comprising:

2 computer-readable program code means for establishing a second secure connection
3 between the PSA and the trusted authenticating domain; and

4 computer-readable program code means for using the second secure connection for the
5 validating of the user.

1 Claim 3 (currently amended): The computer program product according to Claim 1, further
2 comprising:

3 computer-readable program code means for establishing a third secure connection
4 between the PSA and the master registry; and

5 computer-readable program code means for using the third secure connection for the
6 propagating of the received identifying secret to the master registry.

1 Claim 4 (currently amended): The computer program product according to Claim 1, further
2 comprising computer-readable program code means for propagating the received identifying
3 secret to one or more other target registries if the validation succeeds.

1 Claim 5 (currently amended): The computer program product according to Claim 4, further
2 comprising:

3 computer-readable program code means for establishing additional secure connections
4 between the PSA and each of the other target registries; and

5 computer-readable program code means for using the additional secure connections for
6 the propagating of the received identifying secret to the other target registries.

1 Claim 6 (currently amended): The computer program product according to Claim 1, further
2 comprising:

3 computer-readable program code means for obtaining an identification of the trusted
4 authenticating domain from the user during the propagation request processing; and

Serial No. 09/614,087

-4-

Docket RSW9-2000-0074-US1

5 computer-readable program code means for verifying that the trusted authenticating
6 domain is trusted by the master registry as a prerequisite to the propagating.

1 Claim 7 (original): The computer program product according to Claim 1, further comprising:
2 computer-readable program code means for obtaining an identification of the trusted
3 authenticating domain from the master registry.

1 Claim 8 (original): The computer program product according to Claim 6, wherein the master
2 registry stores trust policy information, and wherein the computer-readable program code means
3 for verifying that the trusted authenticating domain is trusted further comprises computer-
4 readable program code means for checking whether the stored trust policy information for the
5 user includes the identification obtained from the user.

1 Claim 9 (original): The computer program product according to Claim 6, wherein the master
2 registry stores trust policy information, and wherein the computer-readable program code means
3 for verifying that the trusted authenticating domain is trusted further comprises computer-
4 readable program code means for checking whether the stored trust policy information for a user
5 group of which the user is a member includes the identification obtained from the user.

1 Claim 10 (original): The computer program product according to Claim 7, wherein the master
2 registry stores trust policy information, and wherein the computer-readable program code means
3 for obtaining the identification of the trusted authenticating domain from the master registry

Serial No. 09/614,087

-5-

Docket RSW9-2000-0074-US1

4 further comprises computer-readable program code means for obtaining the identification using
5 the stored trust policy information for the user.

1 Claim 11 (original): The computer program product according to Claim 7, wherein the master
2 registry stores trust policy information, and wherein the computer-readable program code means
3 for obtaining the identification of the trusted authenticating domain from the master registry
4 further comprises computer-readable program code means for obtaining the identification using
5 the stored trust policy information for a user group of which the user is a member.

1 Claim 12 (currently amended): The computer program product according to Claim 4, wherein
2 the master registry stores password synchronization policy information, and wherein the
3 computer-readable program code means for propagating the received identifying secret to the one
4 or more other target registries further comprises computer-readable program code means for
5 identifying the one or more other target registries using the stored password synchronization
6 policy information for the user.

1 Claim 13 (currently amended): The computer program product according to Claim 4, wherein
2 the master registry stores password synchronization policy information, and wherein the
3 computer-readable program code means for propagating the received identifying secret to the one
4 or more other target registries further comprises computer-readable program code means for
5 identifying the one or more other target registries using the stored password synchronization
6 policy information for a user group of which the user is a member.

Serial No. 09/614,087

-6-

Docket RSW9-2000-0074-US1

1 Claim 14 (original): The computer program product according to Claim 1, wherein the
2 computer-readable program code means for establishing the secure connection further comprises
3 computer-readable program code means for authenticating the PSA to the client.

1 Claim 15 (original): The computer program product according to Claim 2, wherein the
2 computer-readable program code means for establishing the second secure connection further
3 comprises computer-readable program code means for authenticating the trusted authenticating
4 domain to the PSA.

1 Claim 16 (original): The computer program product according to Claim 3, wherein the
2 computer-readable program code means for establishing the third secure connection further
3 comprises computer-readable program code means for authenticating the master registry to the
4 PSA.

1 Claim 17 (original): The computer program product according to Claim 5, wherein the
2 computer-readable program code means for establishing additional secure connections further
3 comprises computer-readable program code means for authenticating the other target registries to
4 the PSA.

1 Claim 18 (currently amended): The computer program product according to Claim 1, wherein
2 the computer-readable program code means for validating further comprises:

Serial No. 09/614,087

-7-

Docket RSW9-2000-0074-US1

3 computer-readable program code means for performing a security function on the
4 received identifying secret of the user, wherein the security function comprises one of (i) a one-
5 way hashing algorithm or (ii) an encryption algorithm;

6 computer-readable program code means for using the received user identifier to locate a
7 previously-stored identifying secret of the user which was stored by the trusted authenticating
8 domain; and

9 computer-readable program code means for concluding that the validation succeeds if the
10 located identifying secret is identical to a result of performing the security function.

1 Claim 19 (currently amended): The computer program product according to Claim 1, wherein
2 the computer-readable program code means for validating further comprises computer-readable
3 program code means for invoking an authenticated LDAP bind or other native authentication
4 mechanism of the trusted authenticating domain, wherein the received identifier of the user and
5 the received identifying secret of the user are passed to the trusted authenticating domain, thereby
6 causing the trusted authenticating domain to validate the passed identifier and identifying secret
7 and return a result which reports a success or failure of the validation.

1 Claim 20 (original): The computer program product according to Claim 1, wherein the PSA has
2 administrative authority for performing operations at the master registry.

1 Claim 21 (original): The computer program product according to Claim 4, wherein the PSA has
2 administrative authority for performing operations at the one or more other target registries.

Serial No. 09/614,087

-8-

Docket RSW9-2000-0074-US1

1 Claim 22 (currently amended): A system for securely propagating security credentials using a
2 trusted authenticating domain, comprising:

3 means for establishing a secure connection between a client and a password
4 synchronization agent (PSA);

5 means for ~~transmitting~~ receiving, at the PSA from the client over the secure connection,
6 an identifier of a user and an identifying secret of the user ~~from the client to the PSA over the~~
7 ~~secure connection~~ during propagation request processing;

8 means for validating the user with the trusted authenticating domain using the ~~transmitted~~
9 received user identifier and identifying secret, on request of the PSA; and

10 means for propagating the received identifying secret of the user directly from the PSA to
11 a master registry if the validation succeeds.

1 Claim 23 (original): The system according to Claim 22, further comprising:

2 means for establishing a second secure connection between the PSA and the trusted
3 authenticating domain; and

4 means for using the second secure connection for the validating of the user.

1 Claim 24 (currently amended): The system according to Claim 22, further comprising:

2 means for establishing a third secure connection between the PSA and the master registry;
3 and

4 means for using the third secure connection for the propagating of the received

Serial No. 09/614,087

-9-

Docket RSW9-2000-0074-US1

5 identifying secret to the master registry.

1 Claim 25 (currently amended): The system according to Claim 22, further comprising means for
2 propagating the received identifying secret to one or more other target registries if the validation
3 succeeds.

1 Claim 26 (currently amended): The system according to Claim 25, further comprising:
2 means for establishing additional secure connections between the PSA and each of the
3 other target registries; and
4 means for using the additional secure connections for the propagating of the received
5 identifying secret to the other target registries.

1 Claim 27 (currently amended): The system according to Claim 22, further comprising:
2 means for obtaining an identification of the trusted authenticating domain from the user
3 during the propagation request processing; and
4 means for verifying that the trusted authenticating domain is trusted by the master registry
5 as a prerequisite to the propagating.

1 Claim 28 (original): The system according to Claim 22, further comprising:
2 means for obtaining an identification of the trusted authenticating domain from the master
3 registry.

1 Claim 29 (original): The system according to Claim 27, wherein the master registry stores trust
2 policy information, and wherein the means for verifying that the trusted authenticating domain is
3 trusted further comprises means for checking whether the stored trust policy information for the
4 user includes the identification obtained from the user.

1 Claim 30 (original): The system according to Claim 27, wherein the master registry stores trust
2 policy information, and wherein the means for verifying that the trusted authenticating domain is
3 trusted further comprises means for checking whether the stored trust policy information for a
4 user group of which the user is a member includes the identification obtained from the user.

1 Claim 31 (original): The system according to Claim 28, wherein the master registry stores trust
2 policy information, and wherein the means for obtaining the identification of the trusted
3 authenticating domain from the master registry further comprises means for obtaining the
4 identification using the stored trust policy information for the user.

1 Claim 32 (original): The system according to Claim 28, wherein the master registry stores trust
2 policy information, and wherein the means for obtaining the identification of the trusted
3 authenticating domain from the master registry further comprises means for obtaining the
4 identification using the stored trust policy information for a user group of which the user is a
5 member.

1 Claim 33 (currently amended): The system according to Claim 25, wherein the master registry

Serial No. 09/614,087

-11-

Docket RSW9-2000-0074-US1

2 stores password synchronization policy information, and wherein the means for propagating the
3 received identifying secret to the one or more other target registries further comprises means for
4 identifying the one or more other target registries using the stored password synchronization
5 policy information for the user.

1 Claim 34 (currently amended): The system according to Claim 25, wherein the master registry
2 stores password synchronization policy information, and wherein the means for propagating the
3 received identifying secret to the one or more other target registries further comprises means for
4 identifying the one or more other target registries using the stored password synchronization
5 policy information for a user group of which the user is a member.

1 Claim 35 (original): The system according to Claim 22, wherein the means for establishing the
2 secure connection further comprises means for authenticating the PSA to the client.

1 Claim 36 (original): The system according to Claim 23, wherein the means for establishing the
2 second secure connection further comprises means for authenticating the trusted authenticating
3 domain to the PSA.

1 Claim 37 (original): The system according to Claim 24, wherein the means for establishing the
2 third secure connection further comprises means for authenticating the master registry to the
3 PSA.

Serial No. 09/614,087

-12-

Docket RSW9-2000-0074-US1

1 Claim 38 (original): The system according to Claim 26, wherein the means for establishing
2 additional secure connections further comprises means for authenticating the other target
3 registries to the PSA.

1 Claim 39 (currently amended): The system according to Claim 22, wherein the means for
2 validating further comprises:

3 means for performing a security function on the received identifying secret of the user,
4 wherein the security function comprises one of (i) a one-way hashing algorithm or (ii) an
5 encryption algorithm;

6 means for using the received user identifier to locate a previously-stored identifying
7 secret of the user which was stored by the trusted authenticating domain; and

8 means for concluding that the validation succeeds if the located identifying secret is
9 identical to a result of performing the security function.

1 Claim 40 (currently amended): The system according to Claim 22, wherein the means for
2 validating further comprises means for invoking an authenticated LDAP bind or other native
3 authentication mechanism of the trusted authenticating domain, wherein the received identifier of
4 the user and the received identifying secret of the user are passed to the trusted authenticating
5 domain, thereby causing the trusted authenticating domain to validate the passed identifier and
6 identifying secret and return a result which reports a success or failure of the validation.

1 Claim 41 (original): The system according to Claim 22, wherein the PSA has administrative

2 authority for performing operations at the master registry.

1 Claim 42 (original): The system according to Claim 25, wherein the PSA has administrative
2 authority for performing operations at the one or more other target registries.

1 Claim 43 (currently amended): A method for securely propagating security credentials using a
2 trusted authenticating domain, comprising steps of:

3 establishing a secure connection between a client and a password synchronization agent
4 (PSA);

5 receiving at the PSA from the client over the secure connection, transmitting an identifier
6 of a user and an identifying secret of the user from the client to the PSA over the secure
7 connection during propagation request processing;

8 validating the user with the trusted authenticating domain using the transmitted received
9 user identifier and identifying secret, on request of the PSA; and

10 propagating the received identifying secret of the user directly from the PSA to a master
11 registry if the validation succeeds.

1 Claim 44 (currently amended): The computer program product according to Claim 1, further
2 comprising:

3 computer-readable program code means for obtaining a new value [[fro]] from the user to
4 be used as the propagated identifying secret if the validation succeeds; and

5 computer-readable program code means for substituting this new value for the received

6 identifying secret prior to operation of the computer-readable program code means for
7 propagating.

1 Claim 45 (currently amended): The system according to Claim 22, further comprising:
2 means for obtaining a new value [[fro]] from the user to be used as the propagated
3 identifying secret if the validation succeeds; and
4 means for substituting this new value for the received identifying secret prior to operation
5 of the means for propagating.

1 Claim 46 (currently amended): The method according to Claim 43, further comprising steps of:
2 obtaining a new value [[fro]] from the user to be used as the propagated identifying secret
3 if the validation succeeds; and
4 substituting this new value for the received identifying secret prior to operation of the
5 propagating step.